Appendix A

National Domestic Communications Assistance Center

Executive Advisory Board

April 11, 2018

Call to Order – Welcome and Introduction
Preston Grubbs, *Chairman*

Introduction of EAB Members & Chairman's Remarks
Preston Grubbs, *Chairman*

Mission & Goals
Preston Grubbs, *Chairman*

NDCAC Update
Marybeth Paglino, *NDCAC Director*

- Review of NDCAC activity since last meeting

Overview of EastWest Institute Report
Kenn Kerns, *Chief Information Officer*
New York County District Attorney's Office

- EastWest Institute (EWI) Report - Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions

Report of the Administrative Subcommittee
Mr. Derrick Driscoll, *Subcommittee Chairman*

- Communications Plan
- Update of ongoing efforts

Report of the Technology Subcommittee
Mr. Michael Sachs, Subcommittee Chairman

- Review of initial meeting
- Summary of subcommittee input

Acknowledgement of Submitted Comments
Preston Grubbs, *Chairman*

Establishing EAB Schedule of Future Meetings
Alice Bardney-Boose, *Designated Federal Officer*

Adjournment

Appendix B

U.S. Department of Justice

National Domestic Communications Assistance Center
Executive Advisory Board
Meeting Minutes
April 11, 2018

NDCAC EAB Members		
Name	**Title**	**Organization**
Alice Bardney-Boose†	Designated Federal Officer	Federal Bureau of Investigation
David Bowers	Inspector in Charge, Security & Crime Prevention	US Postal Inspection Service
Christopher Bubb†	Attorney, Office of the General Counsel (OGC)	Federal Bureau of Investigation
James A Cannon	Sheriff, Charleston County Sheriff's Office	Major County Sheriffs
Thomas Chittum	Chief, Special Operations Division	Bureau of Alcohol, Tobacco, and Firearms
Derrick Driscoll	Assistant Director, Investigative Operations Division	US Marshals Service
Alysa Erichs	Assistant Director, Information Management	Immigration and Customs Enforcement
G. Clayton Grigg*	Deputy Assistant Director, Operational Technology Division	Federal Bureau of Investigation
Preston Grubbs	Assistant Administrator, Operational Support Division	Drug Enforcement Administration
Patrick Haggan	First Assistant District Attorney, Suffolk County DA	National District Attorney's Association
Mark A. Keel	Chief, South Carolina Law Enforcement Division	Association of State Criminal Investigative Agencies
Lenny Millholland	Sheriff, Frederick County Sheriff's Office	National Sheriffs Association
Christopher Noelck	Special Agent in Charge, Investigative Operations, Iowa Department of Public Safety	National Narcotics Officers' Associations' Coalition
Robert Novy	Deputy Assistant Director, Office of Investigations	US Secret Service
Thomas G. Ruocco	Assistant Director/Chief, Criminal Investigations Division, Texas Department of Public Safety	International Association of Chiefs of Police
Michael Sachs	Executive Assistant District Attorney, County of New York District Attorney's Office	Association of Prosecuting Attorneys
Henry Stawinski	Chief of Police, Prince George's County	Major City Chiefs
Peter Winn†	Chief Privacy and Civil Liberties Officer, ODAG	Department of Justice

† Non-Voting Member; *Represented by proxy: Joseph Carrico, Deputy Assistant Director, Operational Technology Division

Appendix C

U.S. Department of Justice

National Domestic Communications Assistance Center
Executive Advisory Board
Meeting Minutes
April 11, 2018

Members of the Public in Attendance

Anthony DiClemente
Nisha Kumar

Appendix D

U.S. Department of Justice

National Domestic Communications Assistance Center

Mission Statement

Mission

To leverage and share the collective knowledge and resources of the law enforcement community to address the challenges involving technical capabilities and solutions, technology sharing, and the implementation of the Communications Assistance for Law Enforcement Act (CALEA) and other legislation; and to strengthen law enforcement's relationship with industry.

Mission Priorities

- Research and assess the communications industry's advancing technology trends and use case scenarios to enhance its knowledge base and identify potential impacts to law enforcement's technical capabilities with respect to:
    - Lawful electronic surveillance capabilities;
    - Evidence collection on communications devices; and
    - Technical location capabilities.
- Leverage research efforts to enhance and promote understanding within the law enforcement community of trends and developments with respect to existing and emerging communications services and technologies.
- Enhance and promote understanding of technical challenges faced by federal, state, tribal, and local law enforcement agencies to advocate on their behalf to relevant decision makers.
- Promote awareness of available tools and capabilities through outreach to law enforcement.
- Provide and facilitate the leveraging of training with respect to industry trends, technical challenges, and viable solutions.
- Develop law enforcement technical needs / requirements documents.
- Facilitate the leveraging and exchange of information and methods among law enforcement and with external partners (e.g., industry) to enhance collaboration.
- Improve relations between law enforcement agencies and the communications industry.
- Promote the adoption of effective law enforcement standard practices.
- Promote awareness of the Communications Assistance for Law Enforcement Act (CALEA) and associated regulations.
- Facilitate the collection of statistical information to illustrate technical challenges associated with lawful electronic surveillance capabilities, evidence collection on communications devices, and technical location capabilities.
- Maintain law enforcement centric customer focus in all support functions and services.
- Understand the necessity to balance law enforcement needs with measures to protect privacy.

U.S. Department of Justice

National Domestic Communications Assistance Center

Mission Statement

Strategic Objectives

Talent

Goal 1: Ensure state-of-the-art technical expertise.

The NDCAC will build technical expertise for the future by ensuring NDCAC personnel are educated on issues involving the changing technology environment.

Objective 1.1: Recruit Talent

- Foster a diverse, accomplished, and conscientious workforce.
    - Assess workforce to identify skills gaps.
    - Ensure recruiting and hiring processes focus on diversity, leadership and closing skill gaps.

Objective 1.2: Nurture Development

- Enable people to learn and grow through involvement in meaningful work.
    - Identify candidates for career development and enrichment opportunities to advance skill sets, provide more career growth opportunities and retain talent.

Objective 1.3: Empower Employees

- Identify problems, develop solutions, and embrace the Mission.
- Promote a culture of accountability and transparency.

Communications

Goal 2: Foster the relationship between law enforcement and communications industry.

The NDCAC will strengthen relationships with various segments of the communication industry through aggressive and coordinated outreach. The outreach program will include educating providers, associations, and others about the difficulties law enforcement faces because of evolving technologies.

Objective 2.1: **Promote Transparency**

- Inform, educate and explain to all stakeholders the "why" and "how" NDCAC's work balances law enforcement needs and privacy.
    - Develop law enforcement training on how to engage with partners.

Objective 2.2: Share Broadly

- Facilitate a culture in which ideas and information are exchanged vertically and horizontally.
    - Assess current communications practices and processes to identify gaps and develop systemic improvements.
    - Assess existing and/or potential new systems to enhance information sharing.

Objective 2.3: Strengthen Partnerships

- Establish working group with members of law enforcement to identify existing barriers to collaboration, as well as identify, leverage, and develop innovative and effective technical solutions.

Capability

Goal 3: Provide valuable assistance and training to the law enforcement community regarding technological advances.

NDCAC personnel will provide state of the art assistance to Federal, State, local, and tribal law enforcement agencies in support of their investigations involving technical capabilities and solutions to lawful electronic surveillance; evidence collection on communications devices; and technical location capabilities. The NDCAC will keep records of the assistance given to requesting agencies and measure the quality of assistance by the degree to which it was considered valuable by the requesting agency.

Objective 3.1: **Maximize Impact**

- Do quality work with an emphasis on exemplary customer service.
  - Measure the timeliness of responses to requests for information and/or technical assistance.

Objective 3.2: Improve Capacity

- Leverage technology to be efficient, enhance performance, sustain access, and mitigate risk.
  - Identify and clarify the technical capabilities and features that law enforcement views as important to accomplishing its mission.
- Enhance knowledge base over time as needs evolve.
  - Assess technological innovations and their impact on Federal, State, local and tribal enforcement agencies and maintain ability to develop solutions and how to deploy them.
- Provide comprehensive curriculum to educate law enforcement on new and emerging services and technologies
  - Leverage existing training opportunities and make them available to law enforcement.
  - Develop in-house training curriculum to fill existing gaps in current training programs relevant to NDCAC mission.

Goal 4: Utilize tools and best practices to maximize the impact of the expenditure of agency funds.

The NDCAC will build capacity within its own ranks by adopting efficiency tools and best practices to ensure wise expenditure of agency funds.

Objective 4.1: Encourage Stewardship

- Use resources wisely and share best practices.
- Foster innovation.
- Embrace ingenuity when evaluating existing policies and practices.

Appendix E

National Domestic Communications Assistance Center

National Domestic Communications Assistance Center (NDCAC)

Program Update

Marybeth Paglino
Director, NDCAC

April 11, 2018

National Domestic Communications Assistance Center

NDCAC Budget

- NDCAC's Fiscal Year Budgets
  - 2018: $10,987,055
  - 2017: $11,441,998
  - 2016: $11,701,998
  - 2015: $12,201,918
  - 2014: $12,201,918 Sequestration Cut
  - 2013: $13,147,740 Annualization
  - 2012: $8,244,000

- The NDCAC's expenditures include:
  - Services
    - Technology Sharing / Tool Development
    - Technical Analysis
    - Solution Verification
    - Technical Resource / Helpdesk
  - Training / Student Expenses and Conferences
  - Outreach
  - Equipment, Facility, Network, and Website

National Domestic Communications Assistance Center

Technical Resource Group

- Provide assistance and technical referrals to law enforcement clients – currently more that 14,600
- Six month trend in number of clients: increase of 1,340
- Types of calls handled by the TRG
  - Access requests for NDCAC services and website
  - Interpretation of provider call detail records / cell tower information
  - Assisting in correlating service provider information
  - Assistance with legal demand (templates)
- Number of requests over the last six months: 3,497

Website

- The NDCAC's Internet presence is composed of two parts
  - Public facing website: general information about the NDCAC and its role
  - Secure portal: restricted access information repository and focal point for law enforcement and industry collaboration
- Challenges with access are being addressed by a multi-factor authentication process
  - New users are being added using the new process
  - To date, 340 users have been added
- Existing users can switch to the new process or continue accessing through LEEP

National Domestic Communications Assistance Center

Communications Applications

- NDCAC has collected information about popular communications applications
  - Type of legal process required
  - Information collected during sign-up
  - Information that may be available from service providers
  - Go-bys
- NDCAC's secure website is a consolidated resource to access information about a growing number of applications
- NDCAC provides training to expand law enforcement understanding of communications applications, to know what applications subjects may be using, and information available from providers

If The Application Is Social Media…

- Social media app providers may have a significant amount of information about subscribers that could prove useful to an investigation
  - Information collected during sign-up
  - Personal profiles
  - Content generated by users (e.g., messages)

- However, providers' records are not necessarily conducive to easy interpretation by law enforcement
  - HTML formatted files consisting of complex folder structure with no way to filter or search a specific time period
  - PDF formatted files
  - Thousands or tens of thousands of pages
  - Single returns for overlapping preservation orders result in duplicate data

National Domestic Communications Assistance Center

How the NDCAC Can Help

- The NDCAC has developed a tool to assist law enforcement in interpreting returns from Social Network providers
- The tool ingests multiple files and parses content and media out of the return, organizes, and makes it searchable
- Exports Social Media returns to Excel compatible files
- Future development will be based on law enforcement input
- NDCAC also provides "Best Practices" training to expand understanding of social media platforms and information available from providers

Open Source Information

- What is it? Information collected from publicly available sources
- How to get it
  - Investigators begin with a general search
  - Different tools often produce different results
- Why is it important?
  - The Internet has become integral to all our lives… and we leave a trail of information with our online activities
  - However, it is critical to streamline, standardize, organize, and maintain records of open source research

How the NDCAC Can Help

- The NDCAC has a tool to search (e.g., names, email addresses, usernames) third party websites, extract relevant data, and organize the information

- Save screenshots and log website information such as page title, URL, and date/time of the information capture for evidentiary purposes

- Simple and intuitive interface and runs in a common browser

Open Source – Training

- NDCAC offers courses for Open Source techniques
  - Learn about tools and methodologies for researching and collecting open source and social media information
  - Become familiar with methods to manage information and authenticate evidence
  - Explore conventional and non-conventional search engines, how they operate, and engines' limitations
  - Identify unique and changing populations of common social networks and find uncommon social networks
  - Learn about operational security - how to mitigate the risk inherent in online investigations
  - Understand the need to institute agency policies and practices designed to balance law enforcement needs with measures to protect privacy

Training

- Since its inception, the NDCAC has provided training to approximately 7,500 law enforcement representatives
  - Onsite classes have hosted more than 1,200 students from 400+ State and local agencies
  - Regional classes have hosted nearly 6,300 students from 1,200+ State and local agencies

- This Fiscal Year, the NDCAC has hosted 1,835 law enforcement representatives
  - 180 onsite students
  - 1,655 students in regional classes

National Domestic Communications Assistance Center

Outreach – Law Enforcement

- The NDCAC continues to proactively reach out and educate the law enforcement community about it's support, tools, and training… in the last six months: nearly 1,700 participants from over 400 agencies

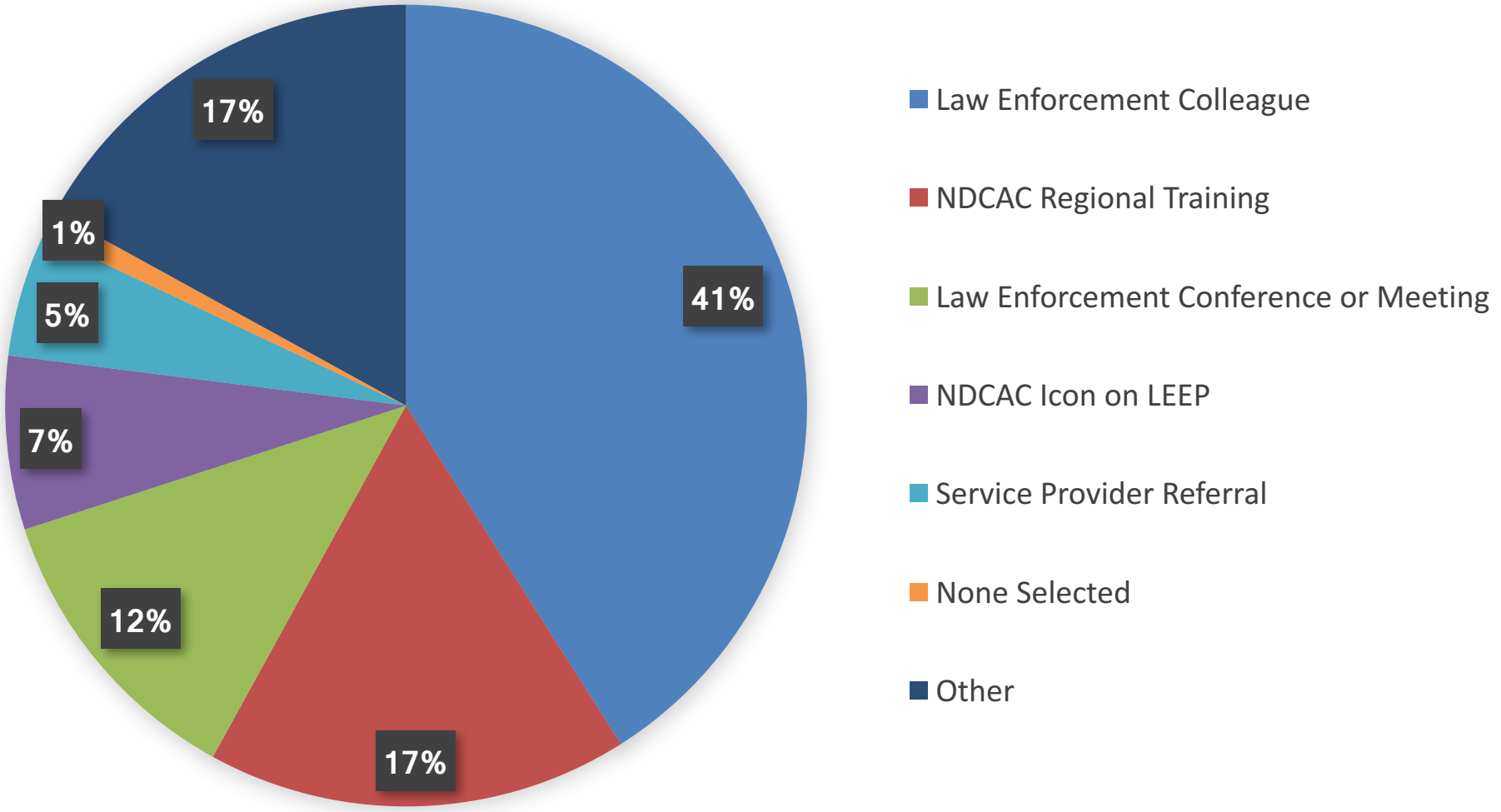
- Proactive Outreach – introduction of the NDCAC and overview of Gathering Evidence from Today's Communication Technologies
  - New York NY
  - Austin TX
  - Charlotte NC
  - San Antonio TX
  - Stafford County VA
  - Myrtle Beach SC

- Participation in established forums
  - Tennessee Gang Investigators Association (TNGIA)
  - International Association of Law Enforcement Intelligence Analysts (IALEIA)
  - Montana Department of Justice
  - Florida Gang Investigators Association (FLGIA)
  - South Carolina Gang Investigators Association (SCGIA)
  - Virginia Crime Analysis Network (VCAN)

National Domestic Communications Assistance Center

Outreach – Law Enforcement

- How law enforcement learns about the NDCAC



Outreach - Industry

- The NDCAC also interacts with industry to gain a better understanding of future services and technologies, how they are implemented, and how they may impact law enforcement

- Attend or monitor industry conferences / meetings that
  - Present new products and features
  - Showcase service-based capabilities
  - Sponsor special interest groups (e.g., abusive messaging and malware)
  - Identify digital forensics and data recovery techniques

- Work with service providers to understand current capabilities, requirements, and future plans for services and deployment of new technologies

- Interact with providers to demonstrate benefits to industry - lessening the burden of addressing similar concerns from multiple agencies
  - NDCAC tools can be used to more easily interpret provider returns

Appendix F

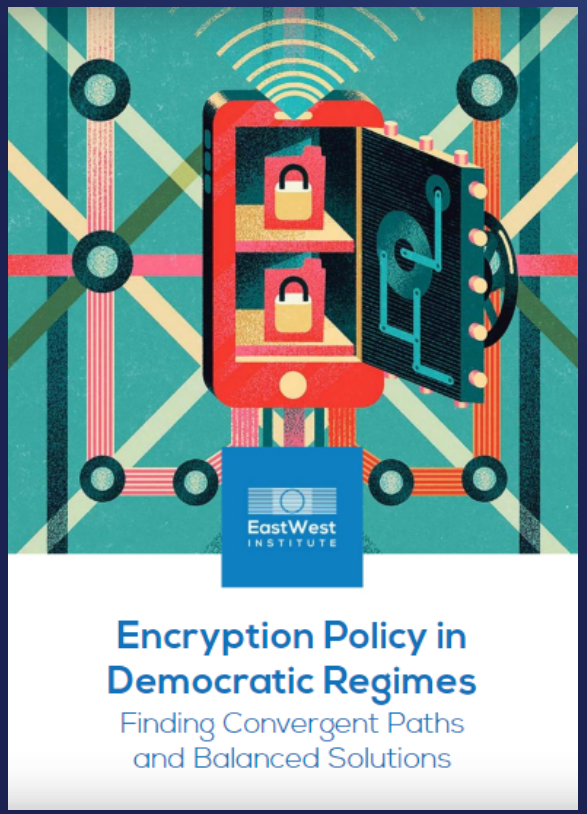
ENCRYPTION

and the IMPACT ON LAW ENFORCEMENT

New York County District Attorney's Office
Presentation to NDCAC Executive Advisory Board

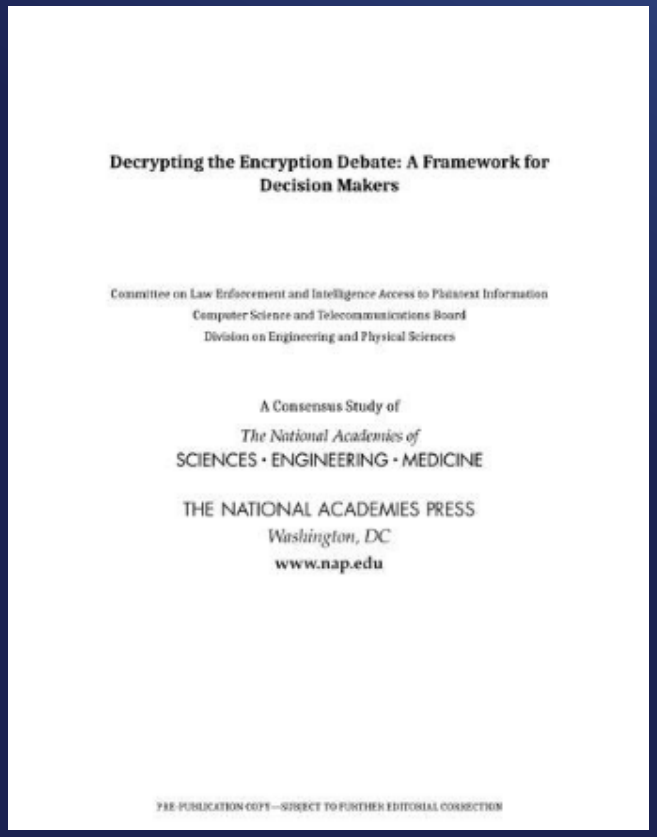
April 11, 2018

National Academy of Sciences & EastWest Institute Reports



- In February 2018, the National Academy of Sciences and East West Institute both issued new reports on the issue of encryption
- The reports discuss privacy and security implications and note that the two interests are not mutually exclusive
- Both publications address the benefits of increased discussion and the need to forge a path forward, past the "technology vs. law enforcement" dichotomy

National Academy of Sciences Report



Decrypting the Encryption Debate: A Framework for Decision Makers

Committee on Law Enforcement and Intelligence Access to Plaintext Information
Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences

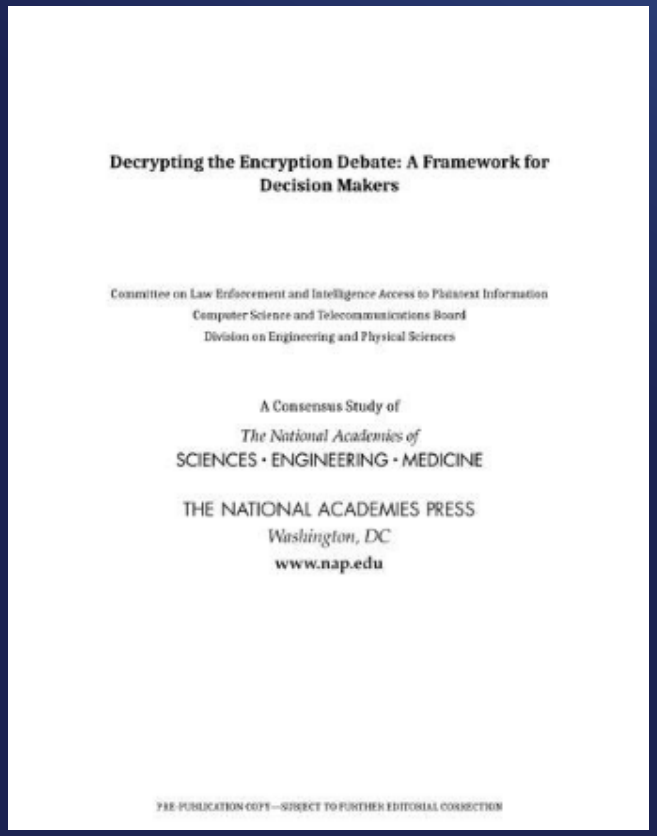
A Consensus Study of
The National Academies of
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS
Washington, DC
www.nap.edu

PRE-PUBLICATION COPY—SUBJECT TO FURTHER EDITORIAL CORRECTION

- 18-month study of the encryption debate
- Committee on Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption:
  - 14 members from academia, technology companies, think tanks, consultants, and law enforcement
  - Tech community representation: Google, Microsoft, Intel
  - Law enforcement representative: Richard Littlehale, Tennessee Bureau of Investigation
  - Chair: Fred H. Cate, law professor and Senior Fellow, Center for Applied Cybersecurity Research, Indiana University

National Academy of Sciences Report



Decrypting the Encryption Debate: A Framework for Decision Makers

Committee on Law Enforcement and Intelligence Access to Plaintext Information
Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences

A Consensus Study of
The National Academies of
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS
Washington, DC
www.nap.edu

PRE-PUBLICATION COPY—SUBJECT TO FURTHER EDITORIAL CORRECTION

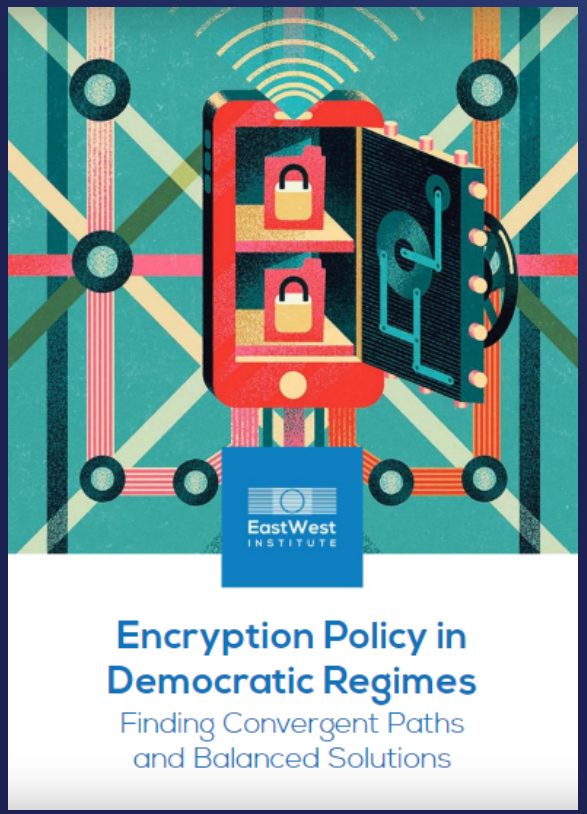
- Highlights technologists ongoing work to develop a device-based solution:
  - Ray Ozzie, Microsoft, former chief software architect
  - Stefan Savage, University of California San Diego, computer science professor
  - Ernie Brickell, Intel, former chief security officer
- Describes tradeoffs of law enforcement access to encrypted content in the current technological landscape
- Provides an eight-question framework for policymakers to consider, with the objective of maximizing effectiveness while minimizing risks
- Our hope is that this report and the framework it presents will cut through the rhetoric, inform decision-makers, and help enable an open, frank conversation about the best path forward."

  - Fred Cate, Committee Chair

National Academy of Sciences Report: Evaluation Framework

1. To what extent will the proposed approach be effective in permitting law enforcement and/or the intelligence community to access plaintext at or near the scale, timeliness, and reliability that proponents seek?
2. To what extent will the proposed approach affect the security of the type of fate or device to which access would be required, as well as cybersecurity more broadly?
3. To what extent will the proposed approach affect the privacy, civil liberties, and human rights of the targeted individuals and groups?
4. To what extent will the proposed approach affect commerce, economic competitiveness, and innovation?
5. To what extent will financial costs be imposed by the proposed approach, and who will bear them?
6. To what extent is the proposed approach consistent with existing law and other government priorities?
7. To what extent will the international context affect the proposed approach, and what will be the impact of the proposed approach internationally?
8. To what extent will the proposed approach be subject to effective ongoing evaluation and oversight?

EastWest Institute Report



- Report created in light of the current "acrimonious" nature of the discussion and entrenched stances
- Advised by EWI Encryption Breakthrough Group
  - Representation from technology sector, law enforcement, privacy advocates
  - Contributors spanning the United States, Europe, and India
- "Encryption provides great benefits and presents challenges, but most stakeholders share common interests in safety and security"

  -Bruce McConnell, EWI Global Vice President
- "Arguments are frequently made that safeguarding information privacy and security are irreconcilable challenges, but they can be complementary"

  - J. Michael Daniel, President and CEO at Cyber Threat Alliance

EastWest Institute Report: Common Interests Frame the Debate

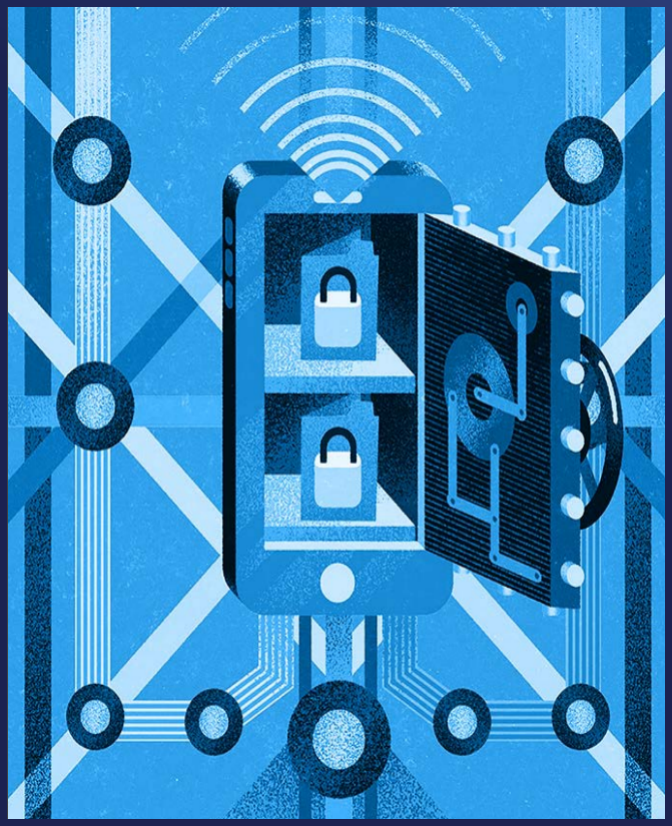
1. Cybersecurity
   - Security of digital information
   - Confidentiality, integrity, availability
   - Increase trust in transactions and data security

2. Law Enforcement and Public Safety
   - Law enforcement access to digital information
   - Crime prevention, detection, investigation prosecution
   - Also holds an interest in cybersecurity

3. Commerce
   - Encourage innovation and efficiency
   - Market-led policies for stronger and user-friendly encryption
   - Benefit of little limitation on country of origin

4. Privacy and Other Human Rights
   - Protect citizens and dissidents from power of authoritarian regimes
   - Encryption as a tool to protect human rights, right to privacy, and freedom of opinion and expression

EastWest Institute Report: Principles



1. Balance Principle: important to find balanced solutions
2. Do-No-Harm Principle: minimize adverse effects and unintended consequences
3. Proportionality Principle: proportion of adverse effects to anticipated gains should be weighed
4. Transparency Principle: greater transparency will increase accountability and public trust
5. Holistic Approach Principle: recognize that encryption is not the only concern for law enforcement
6. Forbearance Principle: need for debate about balanced limits and standards on harnessing new collection approaches
7. Culture Principle: take into account differing cultural values and existing laws

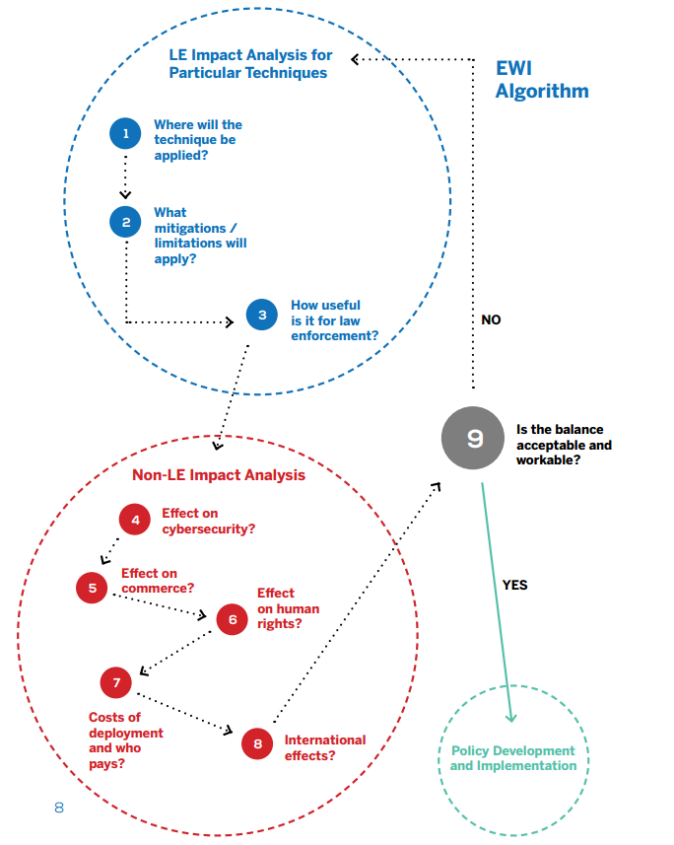
EastWest Institute Report: Assumptions

1. No single solution will solve all problems.
2. Without enacted policy, law enforcement will continue to innovate and seek plaintext.
3. Democratic regimes can devise effective encryption policies that reduce risk of abuse while providing access to law enforcement in some cases (but not risk-free or costless).
4. Human rights cannot be protected if law enforcement is ineffective.
5. Encryption is a serious practical barrier to law enforcement's ability to investigate crimes.
6. Role of encryption in data protection will increase.
7. With Internet of Things, there are increasing data streams available as potential sources of information for law enforcement, but plaintext remains essential.
8. Encryption is not the only barrier, as data may be in unfamiliar formats, outside jurisdiction, or ephemeral.
9. Any technical means that provide lawful access increases risk that criminals will exploit these means.
10. ICT product and service provers should be treated more like telecommunications companies than traditional manufacturers in the security context.
11. Giving law enforcement unrestricted lawful access may lead to abuse.
12. National encryption policies have international ramifications.

EastWest Institute Report

	Regime 1: Lawful Hacking			Regime 2: Design Mandates		
	Data at rest		Data in transit	Data at rest		Data in transit
	Data stored in cloud	Data stored on end device	Commu-nications	Data stored in cloud	Data stored on end device	Commu-nications
Approaches						
Compelled Provider Assistance	●	●	●	●	●	●
Lawful Hacking	●	●	●	Does Not Apply		
Design Mandates	Does Not Apply			●	●	●
Systemic Improvements						
Capacity Building for Law Enforcement (LE)	**Applicable to All Regimes**					
Streamline the MLAT Process						
Enhance LE/Private Sector & International LE Cooperation						

EastWest Institute Report



- Proposes 2 regimes that could enable law enforcement to access encrypted data in limited, legally-authorized cases:
  - "Lawful Hacking"
  - "Design Mandates"

- Provides 9 recommendations for policymakers:
  1. Strong Cybersecurity
  2. Balanced, Transparent, Risk-Informed Regimes
  3. Systemic Improvements
  4. Clear Rules on Compelled Provider Assistance
  5. Limitations on Lawful Hacking
  6. Limitations on Design Mandates
  7. Comprehensive Vulnerability Management
  8. Minimize Data Localization
  9. Periodic Review

Apple and Smartphone Encryption

What we're most commonly asked for and how we respond.

The most common requests we receive for information come from law enforcement in the form of either a Device Request or an Account Request. Our legal team carefully reviews each request, ensuring it is accompanied by valid legal process. All content requests require a search warrant. Only a small fraction of requests from law enforcement seek content such as emails, photos, and other content stored on users' iCloud or iTunes account. National security-related requests are not considered Device Requests or Account Requests and are reported in a separate category altogether.

On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

On devices running iOS 8.0 and later versions, your personal data such as photos, messages (including attachments), email, contacts, call history, iTunes content, notes, and reminders is placed under the protection of your passcode. For all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

Source: https://www.apple.com/privacy/government-information-requests

In September 2014, **Apple** engineered its new mobile operating system, iOS 8, so that it can no longer assist law enforcement with search warrants written for locked devices.

Source: https://www.apple.com/privacy/government-information-requests

Google, maker of the Android operating system, quickly announced plans to follow suit.

Source: http://officialandroid.blogspot.com/2014/10/a-sweet-lollipop-with-kevlar-wrapping.html

Apple and Google's operating systems run a combined **99.3% of smartphones** worldwide.

Source: http://www.idc.com/prodserv/smartphone-os-market-share.jsp

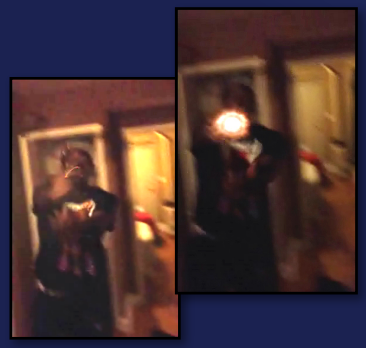
As of January 18, 2018, 93 percent of all Apple devices are running iOS 10 or newer.

Source: https://developer.apple.com/support/app-store

Pre-iOS 8: Real Crimes, Real Victims

Many perpetrators, particularly those who commit sexual offenses, take photos and videos of their acts, and store them on smartphones and computers.

<u>Before Apple's September 2014 change</u>, crucial evidence was obtained from smartphones.



Homicide: People v. Hayes (Pre-iOS 8)

Indictment 04451/2012, New York State Supreme Court

An individual was recording a video on an iPhone when the defendant fatally shot him. The video was used at trial to corroborate eyewitness testimony. The shooter was convicted of murder at trial and sentenced to 35-years-to-life in state prison. If the phone had been encrypted and no one alive knew the passcode, the evidence would be lost.

Criminals are aware of the protection afforded by their encrypted devices.

A defendant in custody for a serious felony told a friend on a recorded jailhouse call that

> "Apple and Google came out with these softwares that can no longer be encrypted [SIC] by the police."
>
> He continued, "If our phones is running on the iO[S] 8 software, they can't open my phone. **That might be another gift from God."**

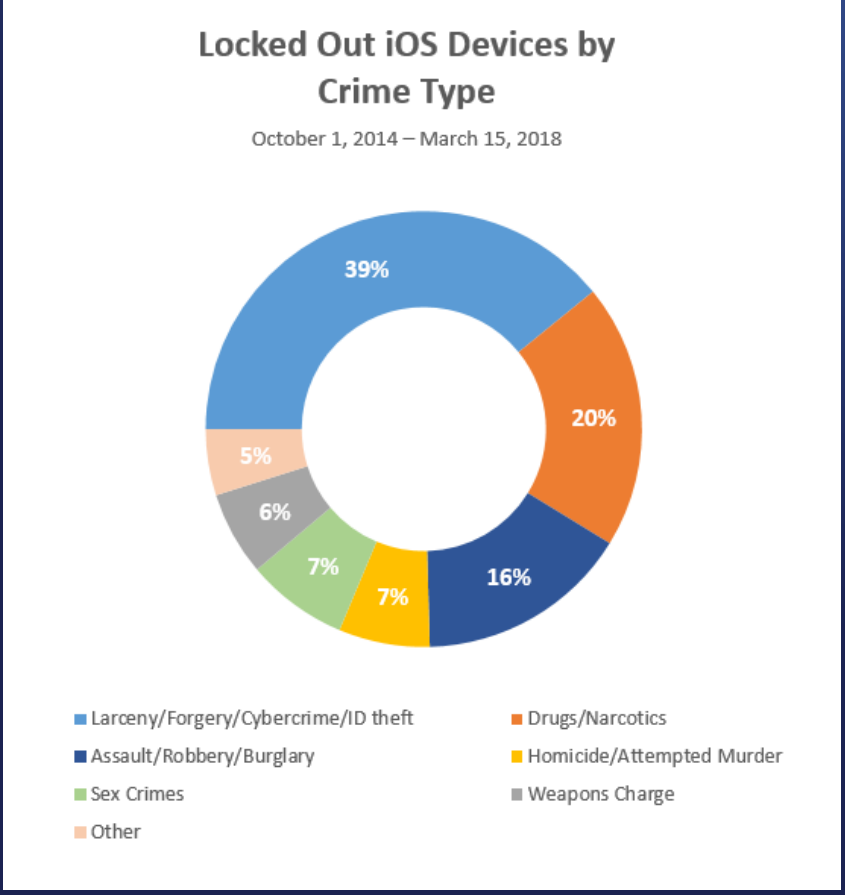
At the Manhattan DA's Office alone, **more than 1,675** iPhones lawfully-obtained since 2014 were inaccessible when they were seized.

Since 2014, **over 73%** of all Apple devices received by our digital forensics unit was locked.

These devices represent hundreds of real crimes against New Yorkers that cannot be fully investigated, including cases of homicide, child sex abuse, human trafficking, assault, cybercrime, and identity theft.

Locked Status Upon Arrival 10/1/14-3/15/18						
	2014	2015	2016	2017	2018	Grand Total
ANDROID						
LOCKED	19	190	259	311	53	832
UNLOCKED	103	322	370	468	87	1350
ANDROID Total	**122**	**512**	**629**	**779**	**140**	**2182**
IOS						
LOCKED	58	382	536	564	135	1675
UNLOCKED	40	143	165	234	30	612
IOS Total	**98**	**525**	**701**	**798**	**165**	**2287**
GRAND TOTAL	**220**	**1037**	**1330**	**1577**	**305**	**4469**

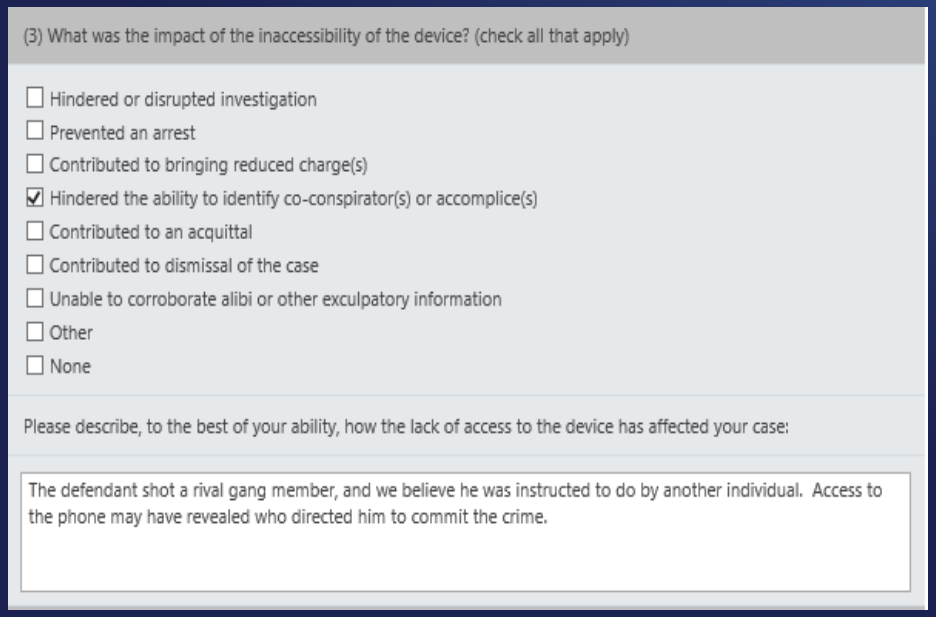
Received Locked Devices by Crime Type



- 7% Homicide/Attempted Murder
- 7% Sex Crimes
- 16% Assault/Robbery/Burglary

Measuring the Effect of Encryption on Cases

Question: What was the impact of inaccessibility of the device?



(3) What was the impact of the inaccessibility of the device? (check all that apply)

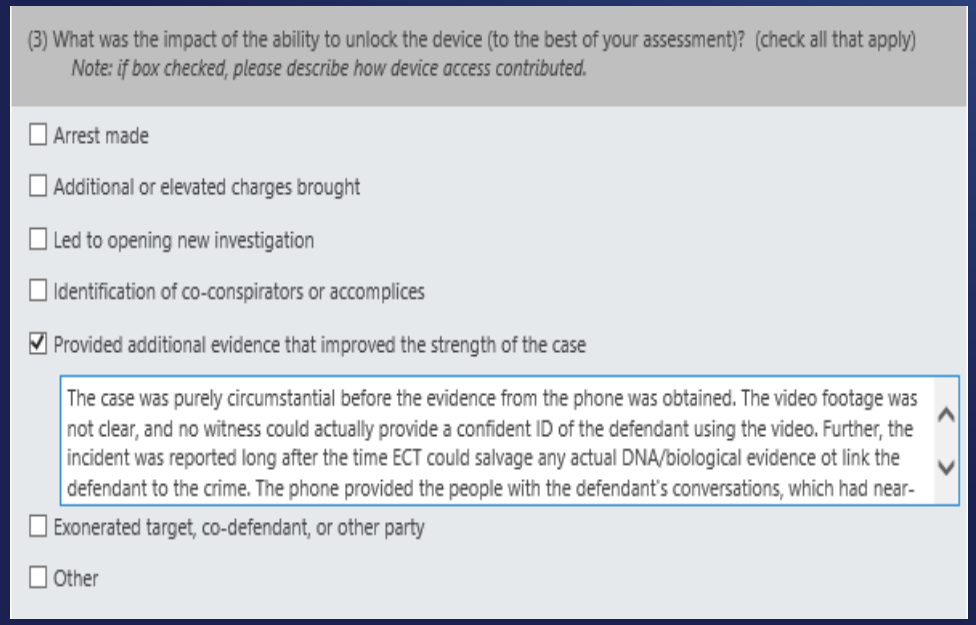
- ☐ Hindered or disrupted investigation
- ☐ Prevented an arrest
- ☐ Contributed to bringing reduced charge(s)
- ☑ Hindered the ability to identify co-conspirator(s) or accomplice(s)
- ☐ Contributed to an acquittal
- ☐ Contributed to dismissal of the case
- ☐ Unable to corroborate alibi or other exculpatory information
- ☐ Other
- ☐ None

Please describe, to the best of your ability, how the lack of access to the device has affected your case:

The defendant shot a rival gang member, and we believe he was instructed to do by another individual. Access to the phone may have revealed who directed him to commit the crime.

- 37.67% hindered or disrupted an ongoing investigation
- 24.16% hindered the ability to identify a co-conspirator

Value of Ability to Access Devices
Question: What was the impact of the ability to unlock the device?



(3) What was the impact of the ability to unlock the device (to the best of your assessment)? (check all that apply)
Note: if box checked, please describe how device access contributed.

- ☐ Arrest made
- ☐ Additional or elevated charges brought
- ☐ Led to opening new investigation
- ☐ Identification of co-conspirators or accomplices
- ☑ Provided additional evidence that improved the strength of the case

The case was purely circumstantial before the evidence from the phone was obtained. The video footage was not clear, and no witness could actually provide a confident ID of the defendant using the video. Further, the incident was reported long after the time ECT could salvage any actual DNA/biological evidence ot link the defendant to the crime. The phone provided the people with the defendant's conversations, which had near-

- ☐ Exonerated target, co-defendant, or other party
- ☐ Other

- 51.14% provided additional evidence
- 17 cases where evidence on a locked phone ultimately exonerated and/or mitigated the culpability of a target or co-defendant

Value of Ability to Access Devices

MURDER

- "This was a murder prosecution. Phone evidence provided (1) motive for crime, (2) partial admission to crime, (3) ability to conduct full investigation into potential cooperator before signing agreement."
- "Phone contained admissions by defendant that he possessed a firearm days before the shooting murder. Phone showed D efforts to hide following the crime. Phone connected D to the individuals captured on video with the murderer at the time of the crime."

Value of Ability to Access Devices

SEX CRIMES & CHILD PORNOGRAPHY

- "From the defendant's phone we obtained 3 videos which constituted CP and we brought a new indictment charging him with Promoting a Sexual Performance by a Child, Use of a Child in a Sexual Performance, Possessing a Sexual Performance by a Child, and Unlawful Surveillance.

  These videos were also strong corroboration of the CW's narrative in which she described the defendant entering her bedroom at night and raping her since the videos were all filmed during the night, in her bedroom, while she was sleeping and unaware."

FRAUD

- "We found audio recordings on the phones that supported our charges that the defendant was intentionally manipulating her victim through fraud and deceit."

Value of Ability to Access Devices: Exoneration / Mitigation

- “Phone corroborated owner's statement that he had not been present when shots were fired”

- “The information in this decedent's phone demonstrated that he died of a voluntary drug overdose.”

- “One video depicts defendant using PCP on night of murder, which is consistent with defense theory of NGRI”

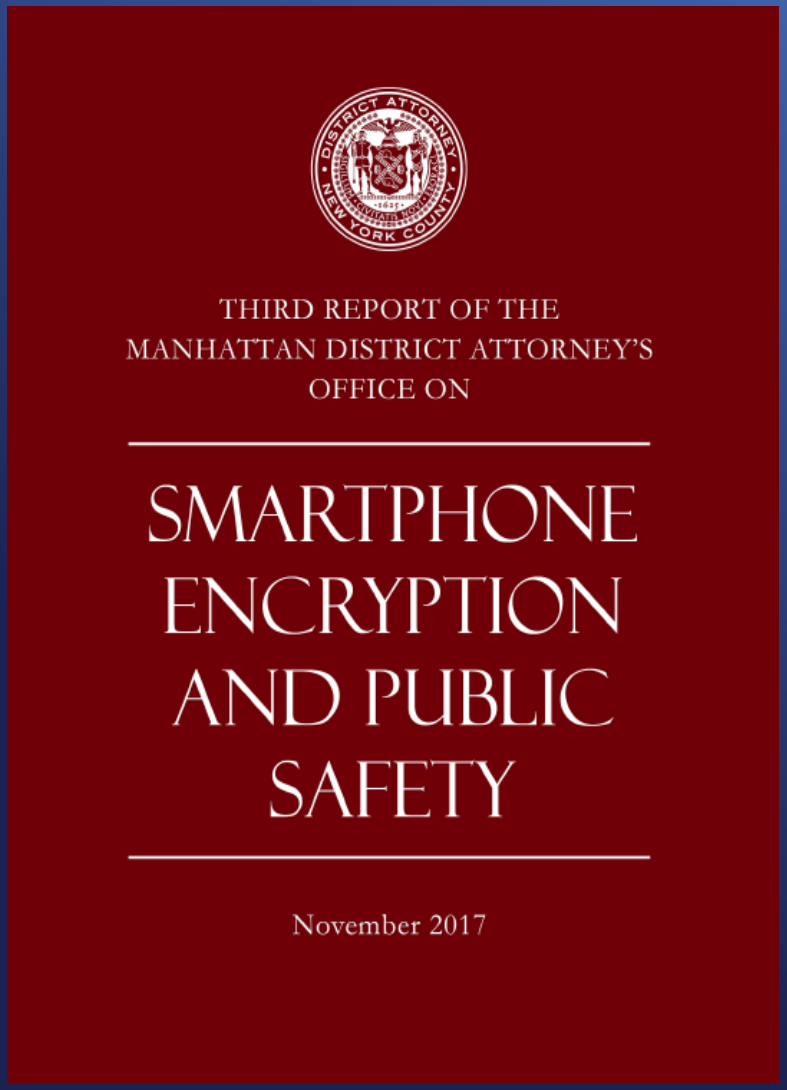
- “Corroborated defendant's statements that he was not present at the time of the crime in a one witness identification case”

Measuring the Effect of Encryption on Cases

- “Defendant and 2 others are alleged to have entered the victim's apartment and robbed him at gunpoint. Our inability to access the contents phone prevents us from seeing who he was in contact with before, during, or directly following the offense. While we can subpoena phone records, there is no other means to access text information or internet based communications such as FaceTime, WhatsApp, Facebook Messenger calls, etc.”

- “Defendant is seen using his phone immediately after the charged murder. Phone may have contained admissions going to defendant's state of mind and his justification defense.”

- “Case investigated by sex crimes as unlawful surveillance, it was reduced to a misdemeanor because we could not access the phone.”


THIRD REPORT OF THE
MANHATTAN DISTRICT ATTORNEY'S
OFFICE ON
SMARTPHONE
ENCRYPTION
AND PUBLIC
SAFETY
November 2017

Kenn Kern

Manhattan District Attorney's Office

Chief Information Officer

(212) 335-4021

KernK@dany.nyc.gov

Appendix G

National Domestic Communications Assistance Center (NDCAC) Communications Plan

March 19, 2018

National Domestic Communications Assistance Center (NDCAC) Communications Plan

(U) INTRODUCTION

(U) The NDCAC was established as a multi-agency center within the Department of Justice to serve as a focal point for technical knowledge management, to facilitate the sharing of solutions and know-how among law enforcement agencies for existing and emerging communications services and technologies, and to strengthen law enforcement's relationships with the communications industry. The FBI serves as the executive agency for the NDCAC, providing necessary technical expertise and day-to-day management of the center, and leveraging the capabilities of other DOJ component agencies.

The mission of NDCAC is focused broadly on challenges with lawfully authorized electronic surveillance, evidence collection from communications providers and devices, and technical location capabilities. Specifically, the NDCAC coordinates Federal, State, local, and tribal law enforcement efforts to address those challenges; leverages and exchanges technical information and support tools among law enforcement agencies; provides technical expertise, training, and advanced capabilities to aid in agencies' lawful intercepts, evidence collection from communication providers and devices, and technical location capabilities; assists in the development of consistent, uniform practices and processes regarding lawful requests for service provider information; facilitates relationships between law enforcement and the communications industry to include leveraging existing relationships and developing new private/public partnerships; assists in the development of law enforcement standard practices; and identifies and tracks trends and developments with existing and emerging communications services and technologies.

(U) The overarching goals of this Communications Plan (Plan) are to increase awareness and understanding about the NDCAC, to communicate with and engage external and internal stakeholders, and to facilitate the transparency of operations to NDCAC staff, stakeholders, and customers. The NDCAC will engage in communications activities with the ultimate goal of increasing the number of clients and the usage of our information and services as well as:

- Communicate the NDCAC mission and vision externally and internally
- Improve information sharing from NDCAC to Federal, State, local, and tribal law enforcement
- Ensure responsiveness to key stakeholders and customers
- Build trust and confidence
- Build support for and understanding of programs, projects, and policies
- Develop high-quality communications materials
- Improve information sharing from executive level management to NDCAC staff
- Institute a continuous feedback loop from all members of the NDCAC community at-large

(U) Strategic communication is the proactive development and delivery of key messages to targeted audiences at the right time using the most effective channels to achieve organizational objectives. "Providing the right people, the right information, at the right time."

(U) There are various types of communications that fall within the scope of this Plan to include: leadership messaging, change communications, communications measurement, stakeholder relationship management, conference planning, and the establishment of technical online forums. The Plan defines the NDCAC communications methods, key messaging themes, stakeholders and evaluation.

(U) COMMUNICATIONS METHODS

(U) NDCAC Overview Presentation

(U) A brief designed to provide both internal and external audiences, with little or no prior knowledge of the NDCAC, a high-level overview of what the NDCAC is, what its mission, vision, goals and objectives are, and what the intended impact of the NDCAC will be on the law enforcement community at large.

(U) Marketing and Communication Materials

(U) These materials, intended for both internal and external audiences, include briefings, tailored emails, brochures, and other publications that can be distributed on a regular or special basis. This type of communication can extend the reach of NDCAC information to subsets of law enforcement that may not have an opportunity to learn about the resources first hand.

- NDCAC tri-fold brochure
- Frequently Asked Questions (multiple editions: e.g., Congress, law enforcement, public)
- Articles written and submitted to law enforcement publications (e.g., IACP's Magazine ["The Police Chief"], NSA's Magazine ["Sheriff"], Law Enforcement Executive Development Association (LEEDA) Magazine ["Insighter"]) - e.g., article about the NDCAC was published in the September 2017 issue of the National Academy magazine
- Newsletters, bulletins, and other periodic programmatic updates
- The NDCAC will produce a high-level overview video of its capabilities (e.g., services, tools, and training) as well as topic-specific informational videos as needed or requested by the law enforcement community (e.g., cell phones at crime scenes).

(U) Law Enforcement Conferences and Meetings

(U) Conference sponsorship / attendance and meetings give both NDCAC leadership and staff an opportunity to spread the message of the NDCAC in a more personal fashion. Forums are beneficial to develop the relationships and trust within the law enforcement community. The NDCAC participates in workshops, training sessions, committee meetings, panel discussions, and presentations. The NDCAC also sets up exhibit space when and where appropriate and feasible. Examples include:

- NDCAC-sponsored conferences and regional outreach meetings
- Law Enforcement Technical Forum
- International Association of Chiefs of Police conferences and meetings (e.g., Police Investigative Operations Committee)
- National Sheriffs Association
- Major City Chiefs Association
- Major County Sheriffs Association
- National Technical Investigator's Association
- Outlaw Motorcycle Gang Investigator's Association
- International Organization of Asian Crime Investigators
- International Associations of Financial Crimes Investigators

- CYBER Crime Investigators
- Association of State Criminal Investigative Agencies (ASCIA)
- National Narcotics Officers' Associations' Coalition (NNOAC)
- Association of Prosecuting Attorneys (APA)
- National District Attorneys Association (APA)
- FBI National Academy Night
- The Annual Dallas Crimes Against Children Conference
- Internet Crimes Against Children Task Force Program

(U) Secure Internet Website

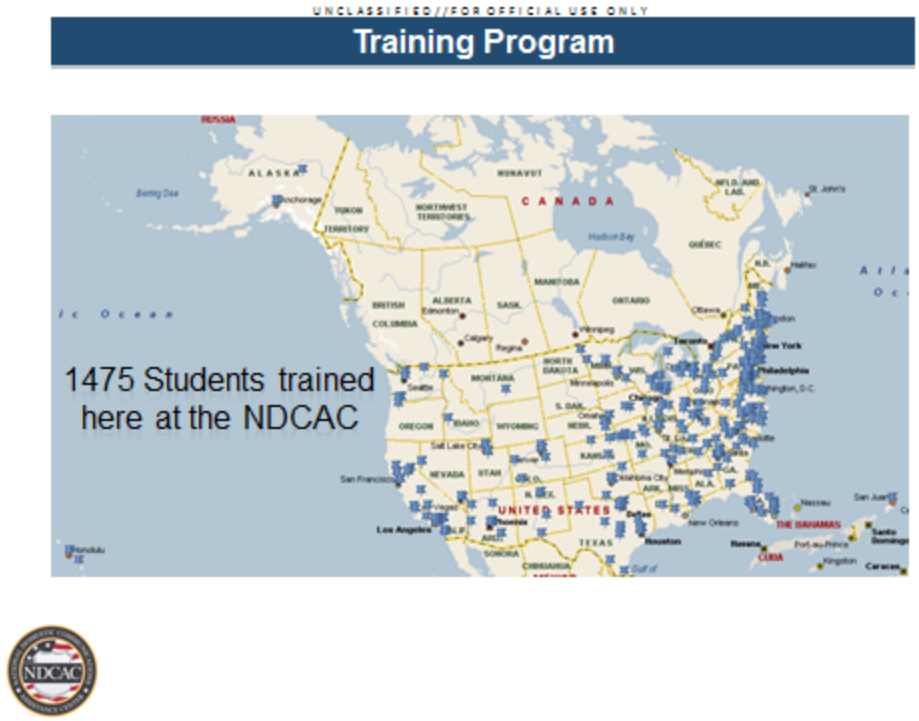
(U) Intended for external law enforcement audiences, the NDCAC's website provides 24/7/365 availability of information content such as protocol updates, communication service provider information, Frequently Asked Questions (FAQs), emerging technologies, and an online reference library for Federal, State, local, and tribal agencies. A complete build-out of the NDCAC Internet website will include a real-time wiki, chat boards, and dedicated repositories for lessons learned documentation from first hand experiences in the field.

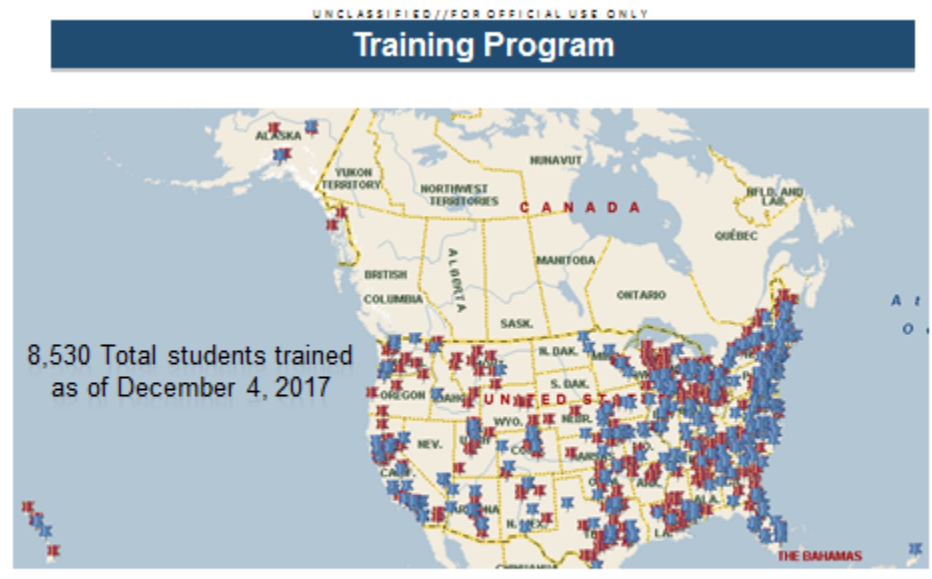
(U) Training

(U) Similar to conferences, attendance by NDCAC staff at law enforcement and/or industry sponsored training, specifically training that targets the core functions of NDCAC, has helped "spread the word" about NDCAC services and technologies and assist in achieving a wider reach into the law enforcement community and private industry. Partnering on training offered by other agencies exposes the NDCAC to different law enforcement audiences – those audiences that would not otherwise know about the services and resources of the NDCAC.

(U) Quarterly Newsletter

(U) These documents, intended for external stakeholders, should provide an overview of the status of operations for the NDCAC. The primary intent of quarterly newsletters is to inform law enforcement of important NDCAC announcements; provide insight into new services, tools, or investigative methods / tips; and garner continued buy-in and support from participating law enforcement agencies. Newsletters can also be tailored to inform industry of the NDCAC's status and benefits to industry of leveraging the NDCAC to communicate with the law enforcement community.

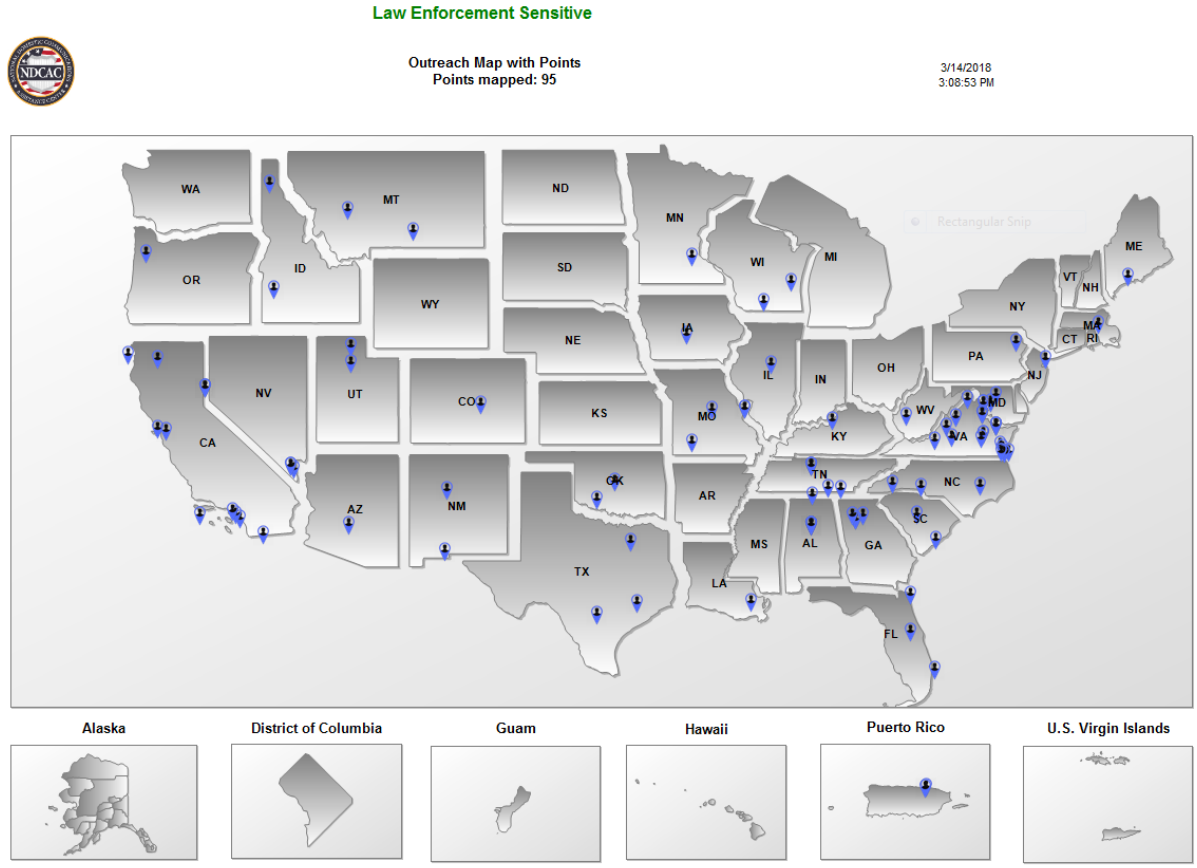




(U) *Outreach*

(U) The NDCAC's law enforcement-centric outreach efforts are designed to create awareness and understanding about the NDCAC and the services and tools it provides; to communicate with and engage stakeholders; and to facilitate the transparency of NDCAC operations to law enforcement customers. To increase awareness of its capabilities, the NDCAC hosts tours for personnel of various Joint Task Forces, law enforcement and prosecutorial

representative associations and organizations; and participates in law enforcement conferences. The NDCAC also sponsors regional training to cultivate the relationship between itself and members of the law enforcement and prosecutorial communities and make them aware of the support provided by the NDCAC.



(U) KEY MESSAGE THEMES

(U) Key message themes ensure consistent communication of NDCAC's goals and program management plans as they pertain to the operating capability of the NDCAC and aid in establishing successful, mutually beneficial services / support to Federal, State, local and tribal law enforcement entities. The key message themes, designed to provide consistent anchors, are reviewed and updated as needed to stay aligned with the organization. Additionally, themes can evolve as changes occur, feedback is received, and lessons learned are incorporated.

(U) The NDCAC will periodically review and alter key message themes as well as perform additional stakeholder analysis.

(U) Key Message Themes for External Audiences

1. (U) The NDCAC is a national center of expertise in lawfully-authorized electronic surveillance capabilities, evidence collection on communications devices, and technical location capabilities.
   a. The NDCAC is a Department of Justice entity with representation on staff from the ATFE, DEA, FBI, and USMS. Its Executive Advisory Board is comprised of representatives from Federal, State, local, and tribal law enforcement and has a State, local, and tribal majority of plus one.

b. Buy-in and ownership of the NDCAC by law enforcement entities at every level is essential to its success.
c. The NDCAC leverages capabilities, knowledge, and research and development from across all levels of the law enforcement community to bring viable technical solutions to the law enforcement community at large.
d. The NDCAC does not take ownership of other agencies' solutions, tools, or training, but acts as a facilitator to highlight agencies' expertise to the law enforcement community.
e. The functions of the NDCAC do not infringe upon the privacy rights of the citizens of the United States.

2. (U) The NDCAC is an integrating mechanism for Federal, State, local, and tribal law enforcement and the communications industry.
   a. The NDCAC sponsors training and conferences aimed at teaching law enforcement and industry best practices in matters of lawfully-authorized electronic surveillance, evidence collection on communications devices, and technical location capabilities.
   b. The NDCAC leverages existing partnerships with Federal, State, local, and tribal law enforcement and utilizes those relationships to gain a greater reach into the community as a whole.
   c. In addition to Federal, State, local, and tribal law enforcement, the NDCAC provides technical training to the prosecutorial community to expand its understanding of the services and technologies impacting law enforcement.
   d. The NDCAC is not designed to replace or inhibit the individual/existing relationships law enforcement agencies may have with industry representatives.
   e. To enhance its ability to assist law enforcement, the NDCAC will be soliciting input from participating agencies and incorporating that feedback into its operations to improve its services, tools, and training.

3. (U) The NDCAC established the Technical Resource Group to provide support related to lawfully-authorized electronic surveillance capabilities, evidence collection on communications devices, and technical location capabilities.
   a. The Technical Resource Group provides assistance to law enforcement personnel in the field and assists in identifying regional law enforcement organizations to leverage local capabilities.
   b. The NDCAC serves as a resource center dedicated to supporting Federal, State, local, and tribal law enforcement cases involving lawfully-authorized electronic surveillance, evidence collection on communications devices, and technical location capabilities.
   c. As of February, 15th 2018 there are 3,267 agencies listed with the TRG with 14,144 users.
   d. In 2017 alone the TRG fielded a total of 5,623 prime tickets, which included requests for solutions for technical questions and services.

(U) Key Message Themes for Internal Staff

1. (U) The NDCAC is a national center with expertise in lawfully-authorized electronic surveillance capabilities, evidence collection on communications devices, and technical location capabilities.
   a. The NDCAC is a first of its kind national asset for law enforcement.

b. The NDCAC leverages best practices from the law enforcement community and industry to provide viable solutions to Federal, State, local and tribal law enforcement agencies across the nation.
c. NDCAC leadership recognizes that its partnerships with Federal, State, local, and tribal governments are critical to the success of its operations.

2. (U) The NDCAC recognizes the role its staff has in supporting law enforcement.
   a. NDCAC subject matter experts have experience at the Federal, State and local law enforcement level and help bridge the gap between the NDCAC and its customers.
   b. The NDCAC contributes to a greater understanding of the challenges faced by law enforcement in the field through its deliberate integration of law enforcement personnel, engineers, and subject matter experts.

3. (U) The NDCAC relies upon the Department of Justice and other inter-agency partnerships as NDCAC activities gain momentum.
   a. Synergy among the ATFE, DEA, FBI, and USMS plays a critical role in the operation of the NDCAC.
   b. The wide array of relationships established by DOJ components and other agencies give NDCAC a wider reach into the State, local, and tribal law enforcement community.
   c. The multi-agency nature of the NDCAC allows it to leverage a wide array of technology, techniques, and procedures for addressing challenges related to lawfully-authorized electronic surveillance capabilities, evidence collection on communications devices, and technical location capabilities.
   d. The Law Enforcement Technical Forum (LETF) is composed of approximately 160 local, state, and federal law enforcement officials who are responsible for their agency technical communications program and/or are technically trained field officers or agents. LETF participants serve as a "think tank" for lawful electronic surveillance and evidence collection expertise for the NDCAC to draw upon and share with all local, state, and federal law enforcement agencies. The NDCAC sponsors two LETF meetings per year. Several LETF members are involved in pilots of NDCAC tools and services and are instrumental in their respective ongoing maturation.

(U) STAKEHOLDER IDENTIFICATION

External Stakeholder	Communications Methods
State, Local, and Tribal Law Enforcement Agencies	Meetings, workshops, conferences, bulletin/newsletter, secure and public website, training, tailored emails, marketing materials
Prosecutorial Community	Bulletin/newsletter, secure and public website, marketing materials, training
Legislative and Regulatory Community	Periodic meetings, public website, outreach, FAQs
Communications Industry	Special bulletins, marketing materials, industry-specific and public website, training, conferences, outreach, workshops, site visits
Press and Advocacy Groups	Press releases, marketing materials, FAQs, public bulletins, website

Internal Stakeholder	Communications Methods
NDCAC Executive Advisory Board	Periodic meetings with the NDCAC Director, bulletin/newsletter, secure and public website, tailored emails
NDCAC Program Managers	Bulletin/newsletter, secure and public website, regular project meetings, emails
NDCAC Staff	
Agency Operational Units	NDCAC overview brief, ELSUR Summit, bulletin/newsletter, marketing materials, emails, meetings, workshops, conferences

(U) Milestones

- High-level overview video of NDCAC capabilities
- Cell phones at crime scene informational video
- Monthly Regional Outreach activities to educate and inform about the NDCAC
- Law Enforcement Conferences and Meetings - as scheduled by associations and other law enforcement groups
- Periodic Newsletter - initially published quarterly
- Semi-annual review of marketing materials (e.g., existing brochures)